Computest
always on.

White paper **Security**

8 security risks at the office that a hacker can exploit

INTRO

In recent years, the issue of security has moved rapidly up the agenda. Virtually every week we read about a big company being hacked, a worldwide malware outbreak or governments collecting exploits in a digital arms race. Fortunately, most organisations are becoming increasingly aware of the risks and are also taking action to better protect their office networks and data.

In recent years, the issue of security has moved rapidly up the agenda. Virtually every week we read about a big company being hacked, a worldwide malware outbreak or governments collecting exploits in a digital arms race. Fortunately, most organisations are becoming increasingly aware of the risks and are also taking action to better protect their office networks and data. Unfortunately, however, there are still enough tricks in the hacker's arsenal to enable them to get inside your network and cause damage anyway. Because even if a door is locked, there's always a window they can get in through.

Table of contents

In this white paper, we give you a glimpse into this arsenal: what can a hacker exploit that the system administrator may not have thought of? Or to put it in another way: if you patch everything properly, run regular updates, have good passwords, install antivirus software and always follow the instruction manual, what vulnerabilities are left for a hacker to exploit? We also give you tools to check for yourself whether your office network is vulnerable to hackers' tricks.

If you want to perform the checks we describe, you'll need a number of tools (all the required download links are also listed separately in the sources). You can also install **'Kali Linux'**: Kali is a Linux distribution that comes with many tools for penetration testing as standard. You can then run Kali as a virtual machine to easily perform the checks. Please note: before you continue, you should be aware that employing many of the tips & tricks we describe here is a criminal offence if you do so without permission or on your own system. Moreover, hacking can also compromise the continuity of the network; so be careful if you are planning to perform checks on production systems!

01 Vulnerability: Notes in Active Directory

Many organisations centralise their authentication and authorisation in order to make user administration easier. This allows an administrator to reset your password or provide access to particular network services from a single central point. The Microsoft version of this service is the most commonly used: Active Directory (AD).

If we look at the nature of the AD, it is an attractive spot for hackers because there is a lot of information there. What many administrators don't know is that the service is accessible to all the users in the network. 'Ordinary' users can also read out a lot of information. Examples of the information which can be obtained are lists of users, registered computers and groups. One of the fields of most interest is the 'notes' field which you can find everywhere. System administrators often use this field to keep notes of information they don't want to forget – for example, why an account was created, what it is used for, and sometimes even the password!

That might seem improbable, but practice suggests otherwise: administrators make the notes in the belief that only they can read them. This is absolutely not the case. If a hacker manages to gain access to an arbitrary AD account (by means of a malware infection or by guessing/cracking the password), he can extract all the information from the AD in order to search for these 'interesting notes'.

Hoe check je dit?

You are now probably asking yourself "am I vulnerable, and how can I check that?" A logical step is to go through all the notes in the AD with your system administrator. What you can also do is use your own account to see what a hacker could have seen. There is a handy tool for this called 'ldapsearch' (see Sources). You can use the following command to look inside your AD:

```
ldapsearch -vv
-o ldif-wrap=no -E pr=1000/noprompt
-D MyAccount@MyDomain -w MyPasswd
-h domaincontroller.domain.local -p 389
-b DC=MyDomain,DC=local > ldapdump.ldif
```

You will need to change 'MyAccount' to your username, 'MyDomain' to the domain of your AD server (this takes the form 'domaincontroller.domain.local') and 'MyPasswd' to your password. As soon as you start the tool, it connects to your AD server and converts all the possible output into a file called 'ldapdump.ldif'. However, this file is not human-readable, so it is useful to convert it into a different format. You can do so using a second tool,

‘ADoffline’. This tool imports all the data in ‘ldapdump.ldif’ into a SQLite database, so you can easily search all the information with queries.

```
python adoffline.py ldapdump.ldif
```

You can then search for interesting information in the file using queries. To open the database, you can use the **‘sqlite3’** tool; you then use the command in conjunction with the database file created. This takes the form ‘sqlite3 ldap.db’, where ldap.db corresponds to the database file. After this you come into the sqlite3 command line where the database is loaded with your AD. There you can use the following sql query to read the notes fields of all users:

```
select sAMAccountName,cn, description, info FROM view_users
WHERE (description IS NOT NUzLL or info IS NOT NULL);
```

02 Vulnerability: Redundant administrator accounts

We all know that admin privileges should not to be used by everyone. There are too many things that can go wrong if these privileges are granted to ‘regular’ users. You cannot assume that those users will know how to use admin privileges responsibly. By giving users limited privileges, you also limit the potential damage that can be done to your IT should a user account become compromised. We often apply this principle to the ‘normal’ users in our organisation, but not to system administrators and IT managers.

One of the most common issues is assigning admin rights to personal accounts which are intended for normal use. As soon as your account falls into the hands of a hacker – for example, as the result of a malware infection – he can exploit it for malicious ends. This also means that a hacker has more privileges on the local system and if you are unlucky, he will even be able to penetrate the network further.

How can you check this?

Checking for redundant administrator accounts is easiest to do in AD: you can see who the administrators are here. Make sure your system administrators always use a regular business account for ‘normal’ work and a separate admin account in their own name for specific administrator work. If you want to understand your risk from a hacker’s point of view, you can also look at how many admin accounts are accessible on your machine locally. Follow these steps to do so.

For this check, we use the tool **‘mimikatz’**. Open the executable to go with your Windows version with administrator privileges (32 or 64 bit). After this, a command line opens. Run the following command:

```
privilege::debug
```

If the output is: ‘Privilege ‘20’ OK’, proceed to the next step. Otherwise, you’ll need to restart the tool with administrator privileges. Now run the following commands one by one to increase your privileges on your machine:

```
token::elevate
token::run
```

You can now try to retrieve all the accounts that have ever been registered with the corresponding authentication methods:

```
sekursla::logonpasswords
```

The output you see is from all the accounts that have ever been logged into this particular machine. You'll see information such as the last login time, which login server was used, but also which login methods are known, with the associated encrypted passwords. A hacker could have got hold of all of this.

03

Vulnerability:

Password theft on the network

Would you believe it if we said your workstation on the network will give up your password just like that? Probably not. However, this is often the case in Windows-based networks where file shares are used over the network.

Suppose you want to connect to "\\network-share1". On the network, your workstation asks 'who is \\network-share1?', hoping for an answer so that it can connect to that server. However, the hacker can also reply before the legitimate server does and say 'Hi, I'm \\networkshare'. Your workstation will then connect to the hacker and try to log in there using your password. The hacker then stops responding, so your workstation will try to reconnect. This time, the hacker lets the legitimate server respond, so you don't even notice that the attack has taken place.

How can you check this?

To check whether your office network is vulnerable to this type of attack, you can use the **'Responder'** tool. This tool listens for and responds to protocols on the network which can be exploited in the attack described above. But please note: this attack interferes with traffic from other users and may be noticed or experienced as disruptive. So we'll give you two versions of the command: the passive and active versions. The idea is to let the tool run for a while to see what comes in. There won't be any output right away. The easiest way to install this tool is on a Debian-based Linux machine using the command 'apt-get install responder'. It is also possible to run the tool on a Windows PC with Python installed on it.

The following command allows you to start the attack. Do make sure 'eth0' is the name of your network interface. Adjust the command accordingly if necessary:

Passivecommand:

```
responder –I eth0 –wF
```

Active command:

```
responder –I eth0 –A
```

If anything is found, you will see it on your screen. And don't worry, the tool also keeps properly sorted logs. These logs are called:

- Responder-Session.log
- Poisoners-Session.log
- Analyzer-Session.log

In the logs, you'll see the encrypted passwords in the form of hashes. These hashes can be exploited using 'Pass-the-hash' (vulnerability 4).

04 Vulnerability: Pass-the-hash attack

When you log in to a Windows service in your network, usually not your password is sent but a derivative of it – a so-called 'hash'. Your password cannot be deduced from this hash, which means anyone who intercepts the hash does not have your password. Sounds safe right?

However, there is a small 'but'. If you authenticate yourself using the hash instead of the password, the hacker doesn't need your password: the hash is enough. This fact is exploited in **pass-the-hash attack**, which have been around since 1997.

The question is how a hacker gets hold of those hashes (and how you can prevent them from doing so). The hacker is primarily interested in hashes belonging to administrators, not those of 'ordinary' users. Once a hacker has access to a workstation, he goes looking for those hashes. There are a number of possibilities:

- Your personal account has more privileges than you need: you are working under an admin account;
- The administrator once physically logged in on your workstation to carry out work activities there: the hash is then stored there;
- The admin account was once logged in remotely: the hash is then stored on your workstation.

If one of these three situations applies, the hacker can exploit the hashes he finds. In more recent Windows configurations, a few obstacles have been erected to an attack of this kind, but the underlying technique continues to apply (now sometimes as **'pass the ticket'** instead of 'pass the hash'). This attack technique was also used in the "NotPetya" **ransomware-aanval van juni 2017** which caused significant damage worldwide. By using this attack technique, NotPetya was very effective at spreading through internal networks: even PCs that had been fully patched were infected.

How can you check this?

You most likely found some hashes or even unencrypted passwords during the previous check. There's already a lot you can do with the unencrypted passwords, but our aim is to exploit the hashes. You can use the hashes to carry out a pass-the-hash attack. We are going to try to use the hashes you have found to connect with a network share. To do so, we are going to use **'crackmapexec'**. Also read the **installatiepagina**.

Use the following command to perform the test. Do replace everything shown between <> with the IP address of the machine, the username of the hash owner, the hash itself and the AD domain. All of this information is available from the check you carried out under vulnerability 2.

```
crackmapexec smb <IP> -u
<gebruikersnaam> -H <LM of NTLM> -d
<domein> --shares
```

Crackmap now uses the hash of the user found for authentication. The attacker doesn't know what the password is. If the attack is successful, you'll see a list of all the possible folders on the machine that you have access to, such as C$, the C-drive.

05 Vulnerability: Use of personal and administrator accounts on services

Systems make use of services in order to perform particular activities. For example, running a backup is performed under an account. These services are supposed to be run under an individual account for security reasons. However, for system administrators it is easier to use their own or admin account during installation. That doesn't matter for the development of the system. However, as soon as the system is taken into production, they often don't think to assign the service an individual account with limited privileges.

How can a hacker exploit this? The login details of the admin account remain on the machine locally, so a hacker who manages to gain control of that machine could immediately acquire more privileges on the network.

How can you check this?
In order to perform this check, we use a tool that comes with Windows. This tool, 'setspn', can only be used in command-line mode. So open a command prompt and enter the following command:

```
setspn -q */*
```

06 Vulnerability: Inactive accounts

The output consists of a number of entries, each of which starts with 'CN='. This is followed by an account name and the services associated with it. The specified CN tells you whether it is a personal account or a service account.

Accounts which have not been in use for some time, such as an account belonging to an ex-colleague, service accounts for old systems or guest accounts, also represent a security risk for the network. Sometimes administrators forget to turn them off. But how much of a risk could that be? Hackers can try to guess the passwords of these accounts. Because the accounts are no longer in use, that will not affect anyone, even if they get locked. What's more, an old account won't have had its password changed in a long time. It is likely that the password will be less strong, particularly if the password policy has since been updated.

How can you check this?
For this check, too, we use 'ldapsearch', because a record is kept in Active Directory of the last time a user logged in. By means of the following ldapsearch query, any user on the network can see which accounts are no longer in use. Don't forget to change the same elements as for vulnerability 1:

```
ldapsearch -vv
-o ldif-wrap=no -E pr=1000/noprompt
-D MyAccount@MyDomain -w MyPasswd
-h domaincontroller.domain.local -p 389
-b DC=MyDomain,DC=local
&(objectClass=User)
(lastLogonTimestamp<=131006038600000000)
(lastLogonTimestamp<=131006038600000000)
```

The long number at the end of the query is an NT timestamp. The number shown in this example stands for 22 June 2016. This number is the limiting value for the accounts you want to display (more information about these timestamps).

07 Vulnerability: Web interfaces of embedded devices

A major risk that is often overlooked are web interfaces of embedded devices such as IP cameras, pedestrian access turnstiles, alarm systems and printers. These devices are often forgotten because they are never actively used. Usually, people are unaware that they are even connected to the network. One of the biggest risks with these devices are the standard login details. These are easy to find online on websites like **defaultpassword.com** or simply on the manufacturer's website. Last year, hackers took advantage of this vulnerability to set up the **'Mirai'** botnet. On 21 October 2016, this botnet took down a quarter of the entire internet, making it the biggest DDoS attack so far.

How can you check this?
Interfaces of embedded devices are easy to find by means of a simple port scan for http and https. For this we use **'nmap'**, a tool that has been used by hackers for years. First we need to know which IP addresses your network is using. You can look this up by looking at your own IP address. Then choose the range that resembles it the most from the list shown below it:

```
192.168.0.0/16
172.16.0.0/12
10.0.0.0/8
```

Then use the following command to scan:

```
nmap –Pn <IP> –p http*
```

Do replace the <IP> with the above IP address you chose. When you enter the command, nmap checks whether there is a webpage that can be requested for each IP. If so, it will tell you. Please note: it can take a little while for the scan to finish.

Sometimes these interfaces are not even protected with a username and password and tempting functionality is directly accessible. If you are prompted to log in, you can often guess the admin password by trying the default password. This default password is often to be found on the manufacturer's website. A list of websites where default passwords are collected is shown under 'sources'.

08 Vulnerability: WPAD proxy service

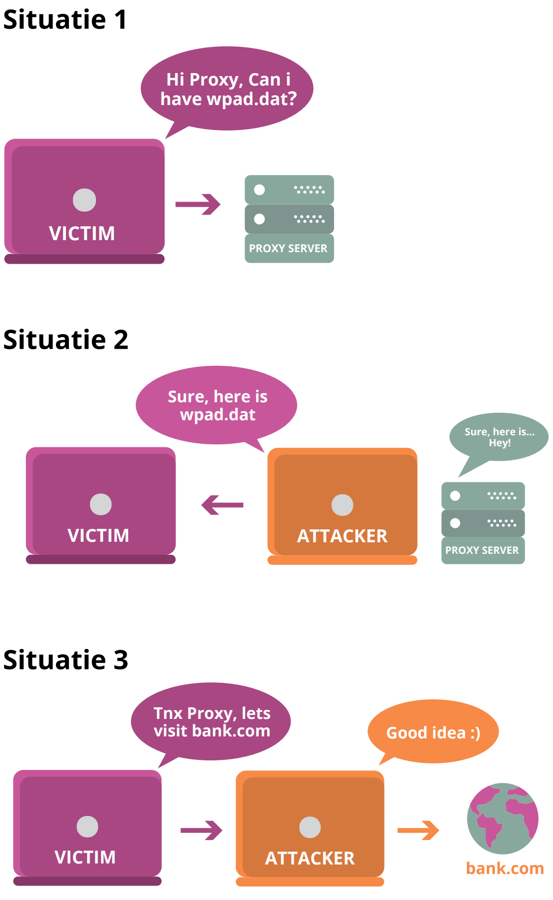
Some office networks have proxies that monitor users' network traffic for added security. This allows administrators to perform additional inspections on network traffic, even on encrypted connections. The drawback of this type of proxy is that all the internet traffic must pass through it and you have to set it up on your own workstation. If you have a lot of workstations on your network, that becomes an impossible task. So you can also do this centrally with a configuration file. Your workstation then only needs to retrieve this file.

The hacker can create a configuration file of this kind himself, inserting his own address. If one of your workstations asks for the configuration file, the hacker can send his own file. This causes all the traffic from that user to go through the hacker's machine. This attack technique is also known as 'man-in-the-middle'. The hacker listens in 'in the middle' of the network traffic and so gets his hands on all your sensitive data. A workstation searches for this type of configuration file using the **'WPAD'**- protocol. The hacker can exploit this protocol to pretend to be a legitimate provider of a proxy configuration file.

Hoe check je dit?

The **'Responder'** tool allows you to check if you are vulnerable to an attack of this kind. You will not obtain output immediately in this check either. It takes a while before you will find anything. When you launch the tool, it responds with a separate configuration file for each WPAD request that it intercepts. The configuration file contains your own IP address. Run the following command to see if you are vulnerable:

```
Responder -w
```


Situatie 1

Situatie 2

Situatie 3

Figuur 1: WPAD aanval

The output you get is the same as for the check for vulnerability 3. Again, the information collected can be used to perform a 'pass the hash' attack as described in vulnerability 4.

09 Conslusion

Constantly keeping the security of your office network up to date is a serious challenge. Hackers get smarter all the time, but fortunately systems do too. However, we cannot expect system administrators to be focused on security daily and always be aware of the latest security breaches. Moreover, many security breaches cannot be resolved simply by following the instruction manual and installing updates and antivirus software. As we have shown, some vulnerabilities are 'tricks' that you need to know, or things you need to systematically integrate into your network configuration.

It is therefore useful to bring in an expert who specialises in the latest attack techniques and actively investigates new vulnerabilities. He or she can help you make your security more robust and stay a step ahead of hackers with smart tricks!

Sources

Tools

Most of the tools can be found in the Kali Linux distribution: https://www.kali.org/downloads/

You can also download and run the tools individually. Do bear in mind that a virus scanner may get triggered by them. A hacker will devise ways around that, but for the purposes of evaluating your own security it is easier to tell the virus scanner that these tools are authorised.

If you are using a different Linux distribution than Kali, it is worth first checking to see if the tools are already available in the distribution's package management system before you start downloading and installing them yourself. Tools like 'ldapsearch' and 'sqlite3', for example, you can get via your package manager (e.g. apt-get and yum for Debian-based and Redhat-based systems, respectively).

Crackmapexec:
https://github.com/byt3bl33d3r/CrackMapExec/wiki/Installation
Responder:
https://github.com/lgandx/Responder
ADoffline:
https://github.com/stufus/ADOffline
Nmap scanner:
https://nmap.org/
Mimikatz:
https://github.com/gentilkiwi/mimikatz/releases
Default password websites
http://www.routerpasswords.com
http://www.defaultpassword.com
https://cirt.net/passwords
Documentatie
Active directory:
https://nl.wikipedia.org/wiki/Active_Directory
NTLM en authenticatie documentatie:
https://technet.microsoft.com/en-us/library/hh994565(v=ws.11).aspx
https://technet.microsoft.com/en-us/library/bb457114.aspx

TN timestamp converter:
https://www.epochconverter.com/ldap
SAM, Security Account Manager:
https://en.wikipedia.org/wiki/Security_Account_Manager
Proxy:
https://nl.wikipedia.org/wiki/Proxyserver
WPAD:
https://en.wikipedia.org/wiki/Web_Proxy_Auto-Discovery_Protocol
Hash:
https://nl.wikipedia.org/wiki/Hashfunctie
Pass the hash:
https://en.wikipedia.org/wiki/Pass_the_hash
https://www.hacking-lab.com/misc/downloads/event_2010/daniel_stirnimann_pass_the_hash_attack.pdf
https://attack.mitre.org/wiki/Technique/T1097
Responder demo youtube:
https://www.youtube.com/

More information?

Want to know more about how you can protect your office network from attackers, or need help performing these checks? Our ethical hackers will be happy to help. You can contact them with no obligation at **info@computest.nl**. Want to read more? **Click here** for a list of our security and performance white papers.